# EXHIBIT F

Privacy Impact Assessment
for the

# Airport Access for Aviation Workers

**DHS/TSA/PIA-020(c)**

**April 27, 2020**

**Contact Point**
**Sonya Badgley**
**Enrollment Services and Vetting Programs**
**Transportation Security Administration**
**Aviation.Workers@tsa.dhs.gov**

**Reviewing Official**
**Dena Kozanas**
**Chief Privacy Officer**
**Department of Homeland Security**
**(202) 343-1717**

## Abstract

The Transportation Security Administration (TSA) conducts security threat assessments on individuals working at airports. These include individuals seeking or holding authorized airport access or airport identification badges or credentials, as well as identification credentials or badges recognized by TSA under 49 CFR Parts 1542 and 1544, and non-traveling individuals requiring unescorted access to the sterile area of the airport.[1] Additionally, Congress, through the Federal Aviation Administration (FAA) Reauthorization Act of 2018, directed TSA to establish a national centralized database containing the names of individuals who have had an airport and/or aircraft operator-issued credential or badge revoked for failure to comply with aviation security requirements. This Privacy Impact Assessment (PIA) consolidates and supersedes earlier PIAs regarding aviation worker security threat assessments (STA) published in 2004, 2005, and 2008 and discusses the creation of the new national centralized database.

## Overview

The TSA conducts security threat assessments on a wide variety of individuals who seek authorized access to airports in order to work or perform other authorized functions. An STA is an inquiry to confirm an individual's identity and determine whether the individual poses or may pose a security threat to transportation or national security, or threat of terrorism. This PIA does not cover aviation passenger vetting, which is performed under the Secure Flight program.[2] TSA does not issue identification badges or credentials for aviation workers; that function is performed by the local airport authority. Some airports may also recognize identification badges issued by other issuing authorities (such as badges issued by tenant companies, aircraft operators, or foreign air carriers located on the airport), or may choose not to issue any badge or credential at all but require an STA for individuals who work at the airport.

Airports have widely divergent security needs for the workforces that perform duties at an airport, which may include authorizations for access to public areas as well as controlled areas. For example, airports may authorize work access for individuals performing functions such as landscaping or construction, ground transportation, restaurants, stores, facilities maintenance, inspections, delivery services, servicing concessions, aircraft carrer ticket counters, boarding gates, or maintenance and fueling of an aircraft. Airports may also permit non-traveling individuals to access the sterile area to accompany a minor to the gate, go shopping at stores located in the secured area, or perform routine inspections or maintenance.

---

[1] "Sterile area" is defined as a portion of the airport defined in the airport security program that provides passengers access to boarding aircraft and to which the access generally is controlled by TSA, or by an aircraft operator under part 1544 of this chapter or a foreign air carrier under part 1546 of this chapter, including the screening of persons and property. 49 CFR 1540.5

[2] *See* DHS/TSA/PIA-018 Secure Flight Program, *available at* https://www.dhs.gov/privacy.

In general, an STA may contain a check of intelligence databases for terrorism or related concerns, such as Transnational Organized Crime (TOC); a criminal history record check; and a check of immigration databases to confirm lawful presence. The Appendix to this PIA provides more specific details on the STA required under different access programs. The STA is performed on a recurrent basis in order to provide the most current level of information on potential security threats.

Individuals whose STA includes a fingerprint-based criminal history record check (CHRC) are enrolled by the airport operator in the Federal Bureau of Investigation's (FBI) Record of Arrests and Prosecutions (RAP) Back Program for recurrent vetting. RAP Back is a program under the FBI Next Generation Information (NGI) system that enables a participating airport operator to receive ongoing status notifications of any subsequent criminal history information changes reported on individuals who have been enrolled with RAP Back.[3] In addition, TSA will enroll individuals with the Department of Homeland Security (DHS) Office of Biometric Identity Management (OBIM) Automated Biometric Identification System (known as IDENT)[4] for recurrent checks against immigration, terrorism, and law enforcement holdings in that system. IDENT is a DHS-wide system for the storage and processing of biometric and biographic information for DHS mission-related functions. TSA will enroll individuals in IDENT's successor system, the Homeland Security Advanced Recognition Technology (HART), once it is developed.

TSA also expects to share personally identifiable information (PII) from covered aviation workers with the DHS Data Services Branch. Formerly the DHS Data Framework, the DHS Data Services Branch is the Department's solution to enable authorized users to search datasets extracted from multiple DHS systems to view information in an accessible format. Further information about the DHS Data Services Branch can be found in its PIA.[5]

*Data flow for Airport Worker Vetting*

Under the current vetting process, TSA and airport operators share responsibility for the vetting of airport workers. For individuals who need access to the Security Identification Display Area (SIDA), sterile area, or Air Operations Area (AOA),[6] or receive an identification badge or

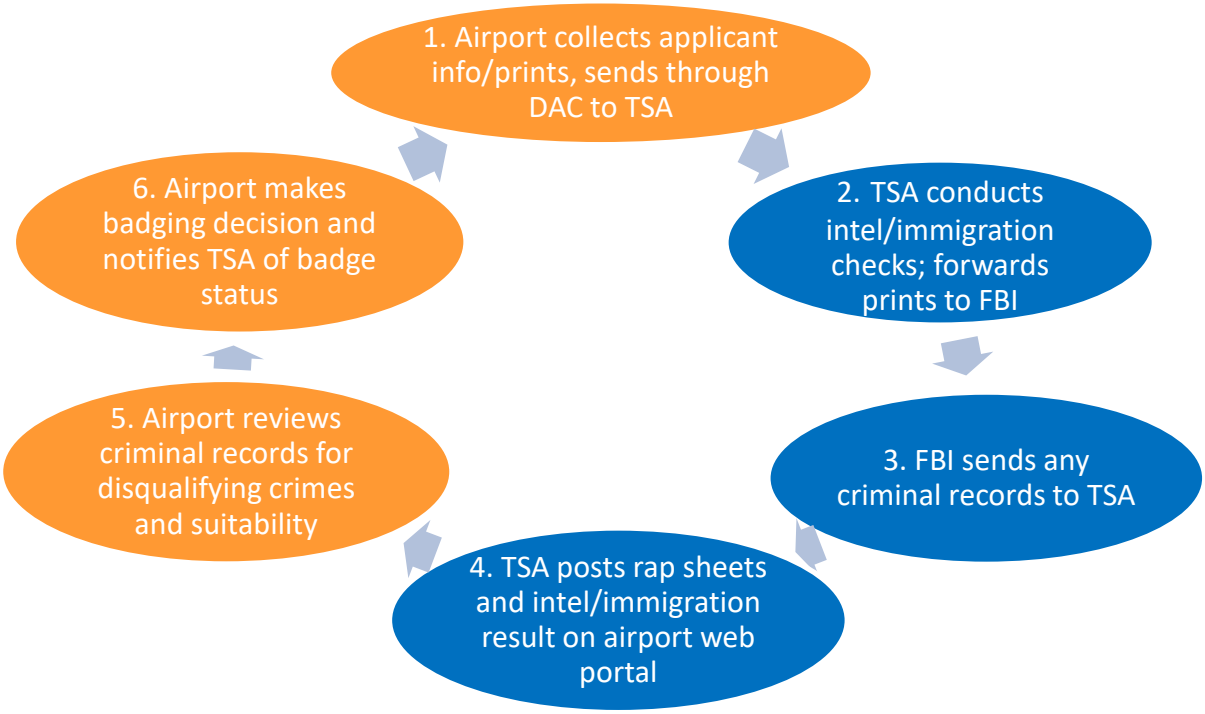
[3] For more information about the FBI Rap Back Program, please *see* Privacy Impact Assessment for the Next Generation Identification - Rap Back Service, *available at* https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments.
[4] *See* DHS/OBIM/PIA-001 Automated Biometric Identification System (December 7, 2012), *available at* https://www.dhs.gov/privacy.
[5] *See* DHS/ALL/PIA-046(e) DHS Framework (October 6, 2017), *available at* https://www.dhs.gov/privacy.
[6] Air operations area (AOA) means a portion of an airport, specified in the airport security program, in which security measures specified in 49 CFR 1540.5 are carried out. This area includes aircraft movement areas, aircraft parking areas, loading ramps, and safety areas, for use by aircraft regulated under 49 CFR Part 1544 or 1546, and any adjacent areas (such as general aviation areas) that are not separated by adequate security systems, measures, or procedures. This area does not include the secured area. 49 CFR 1540.5.

credential to work in the public area[7] of the airport, the airport's Designated Aviation Channeler (DAC)[8] collects the individual's biographic information, transmits it to TSA, and TSA conducts the intelligence and immigration checks. If TSA determines that an applicant may pose a threat to security or is not in the United States lawfully, TSA requires the airport to deny the badge for that applicant. For the CHRC, the airport collects fingerprints from airport workers and submits them through the DAC to TSA, which then submits them to the FBI. The FBI returns any rap sheets associated with the fingerprints to TSA, and TSA posts them on a web portal for airports to access and adjudicate their respective applicants' criminal history. Airport operators can view only rap sheets for their own applicant. Airport operators compare an individual's rap sheet against the list of disqualifying crimes with their associated look-back period, and may issue credentials if there is no conviction for a disqualifying crime.[9] In addition, an airport operator may disqualify an applicant due to its own employment suitability factors that are not necessarily related to transportation security. On these matters, the airport operator makes the final decision to issue a credential.

Figure 1 illustrates the flow of information for individuals who need SIDA or sterile area identification media. This group typically includes individuals who work at restaurants and shops located beyond the screening checkpoint in the sterile area; airline mechanics and baggage handlers who work on and around aircraft; airline pilots who hold a SIDA at their home airport; and airport badging office employees who need access to or may be located in the SIDA.

[7] For the purposes of this PIA, TSA considers the public area to be all non-49 CFR Part 1542 regulated areas on the airport property.
[8] Designated Aviation Channelers are contractors approved by TSA to collect and transmit biographic and biometric information from individuals who are required to undergo security threat assessments and submit to TSA on behalf of airport operators.
[9] 49 U.S.C. § 44936; 49 CFR 1542.209(d).

**Figure 1: Airport Worker Vetting**




For airline employees working at the airport, air carriers typically conduct the CHRC and certify to the airport that the individual passed the CHRC. Based on this certification, the airport issues the SIDA credential. The air carriers conduct No Fly/Selectee List checks of employees, rather than the Terrorist Screening Database (TSDB) check TSA conducts on airport workers.[10] TSA has begun efforts to transition the responsibility for conducting these checks away from the airlines in order to reduce risks posed by sharing watch list information with airport and aircraft operators. Once transitioned, airport operators and aircraft operators will no longer conduct the No Fly/Selectee List check for direct employees and authorized representatives, including those who do not work at an airport and have not been issued an airport badge but do require access to sensitive information, such as reservation agents.

Employees at airports that do not have a secured area or a badging system must still be vetted. These employees typically work at small airports that employ only a few individuals and have no formally defined secured areas, SIDA, or badging system. In order to comply with the STA requirement, the security manager at these small airports must obtain an STA and CHRC via TSA Pre✓® or a Known Traveler Number (KTN) under another U.S. Government Trusted

[10] This practice will change when TSA migrates all remaining watch list vetting functions from aircraft operators back to TSA, and TSA will conduct a full TSDB check on these individuals rather than the current No Fly/Selectee checks currently performed by aircraft operators.

Traveler Program, such as Global Entry, NEXUS, or SENTRI, in order to be vetted.[11] Because of the small numbers and lack of a DAC for access, the security manager sends the PII necessary for the STA to TSA via email. TSA submits these records into its Transportation Vetting System (TVS)[12] for recurrent vetting, and communicates the result with the airport by password protected email.

Non-traveling individuals visiting small airports, such as those accompanying a passenger, maintenance workers, or other visitors requiring a gate pass, are vetted through TSA's e-Secure Flight platform.[13] This system permits short-term visitors to be vetted without conducting recurrent checks for a long period of time. Small airports may choose to use the e-Secure Flight platform for vetting their employees instead of using email. TSA is working on creating a secure portal to TVS through which the aircraft operators and small airports may securely transmit their employees' PII to TSA to replace the email transmission method.

*Centralized Database for Revocations*

Congress has directed TSA to establish a national centralized database containing the names of individuals who have had an airport and/or aircraft operator-issued credential or badge revoked for failure to comply with aviation security requirements.[14] Airport and aircraft operators will be required to enter the name, SSN, contact information, and airport location of individuals who meet the reporting criteria into the database, and all airport and aircraft operators will be required to query the database when determining level of access. The database will assist airport operators to manage risks from aviation workers who move from one airport to another after committing security violations that result in their credential or badge being revoked. Airport and aircraft operators must provide the opportunity for redress to individuals entered into the centralized database so that the individual can challenge his or her inclusion in the database.

# Section 1.0 Authorities and Other Requirements

## 1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

49 U.S.C. § 114(f); 49 U.S.C. § 44936. TSA has issued regulations implementing this authority with reference to airport and airline operators at 49 CFR Parts 1542 and 1544, respectively. The FAA Reauthorization Act of 2018, Section 1934(i), requires the creation of the

[11] For more information on CBP's Trusted Traveler Programs, please *see* DHS/CBP/PIA-002 Global Enrollment System (GES), *available at* https://www.dhs.gov/privacy.
[12] TVS is the currently the primary system for performing security threat assessments. TVS is identified in DHS/TSA/PIA-042 as a feeder system to Technology Infrastructure Modernization (TIM). All PII contained in TVS is discussed in the program PIAs that cover the data collected. For example, aviation workers are covered under this PIA.
[13] *See* DHS/TSA/PIA-018(h) Secure Flight Program, *available at* https://www.dhs.gov/privacy.
[14] FAA Reauthorization Act of 2018, Section 1934(i).

centralized database for individuals whose airport credential has been revoked for violations of aviation security requirements.

### 1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The following SORNs apply:

- DHS/TSA-002 Transportation Security Threat Assessment System (TSTAS),[15] which covers individuals who undergo a security threat assessment, employment investigation, or other evaluation performed for security purposes or in order to obtain access to transportation infrastructure or assets; and
- DHS/TSA-019 Secure Flight Records,[16] which covers the non-traveling individuals who seek to obtain authorization from an aircraft or airport operator to enter the sterile area of an airport.

### 1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes, information in TSA's information technology systems is safeguarded in accordance with the Federal Information Security Modernization Act (FISMA), which establishes government-wide computer security and training standards for all persons associated with the management and operation of federal computer systems. The TSA systems associated with this PIA are operating on the authority of the Designated Accrediting Authority (DAA). TSA's Technology Infrastructure Modernization (TIM) program[17] was certified and accredited on March 12, 2014, and has been re-certified and re-accredited during the intervening time.

### 1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes, NARA approved the records retention schedule covering the STA process in August 2013 (N1-560-06-6; DAA-0563-2013-0001-0008, 0009, 0010). TSA is currently seeking NARA approval for the records retention schedule for the centralized database.

### 1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an

[15] DHS/TSA-002 Transportation Security Threat Assessment System, 79 FR 46862 (August 11, 2014).
[16] DHS/TSA-019 Secure Flight Records, 80 FR 233 (January 5, 2015).
[17] *See* DHS/TSA/PIA-042 TSA OIA Technology Infrastructure Modernization Program (March 26, 2014), *available at* https://www.dhs.gov/privacy.

**appendix.**

Yes. The following collections are part of this overall Airport Access for Aviation Workers security threat assessment process:

| | |
|---|---|
| Airport Security Program | OMB Control Number 1652-0002 |
| Aircraft Operator Security Program | OMB Control Number 1652-0003 |
| Centralized Database | *New collection |

# Section 2.0 Characterization of the Information

## 2.1 Identify the information the project collects, uses, disseminates, or maintains.

TSA collects the following information on individuals to conduct STAs:

- Full name;
- Other names used
- Gender;
- Date of birth;
- Place of birth;
- Height;
- Weight;
- Hair and eye color;
- Race;
- Social Security number (SSN),[18]
- Citizenship,
- Driver's license or other identity document (e.g, Passport number and country of issuance, if applicable);
- Lawful presence (date of naturalization, the type, number and expiration date of visa, if applicable), or other documentation adequate to establish immigration status (alien

[18] SSN is voluntary unless seeking SIDA access. SIDA access applicants must provide SSN per Section 1934(c) of the FAA Reauthorization Act of 2018.

registration number (A-Number) or Form I-94 Arrival/Departure Number, or certificate of naturalization number or certificate of birth abroad);

- Current mailing address and mailing address for preceding five years;
- Current residential address and residential address for preceding five years; email address unless individual does not have one; phone number;
- Submitting entity and business contact information (i.e., current employer or prospective employer's address, airport code, phone, and facsimile numbers);
- Individual's employer information;
- Business contact information for the preceding five years; and
- Fingerprints (When required for the credential)

TSA will maintain the results of the STA and any underlying information supporting the result, as well as information submitted by individuals seeking redress.

The centralized database for revoked badges will maintain the individual's name, SSN, contact information, airport location that revoked access, and the reasons for the revocation, as well as any submission by the individual seeking correction of his or her record.

## 2.2 What are the sources of the information and how is the information collected for the project?

Aviation workers provide their information to their aircraft operator, the airport's DAC, or airport security manager or security office. Aircraft operators will transmit their direct employees' and authorized representatives' information directly to TSA. In addition, the system may also include information originating from the intelligence, immigration, or law enforcement databases queried as part of the STA, and results of the CHRCs and IDENT checks. TSA may also conduct searches of open sources, including publicly available social media, as part of the STA review as described in Section 2.3 below. Airport operators will provide information for the centralized database on individuals with revoked badges.

## 2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

The vetting of aviation workers does not involve information from commercial sources or publicly available data for most of the individuals being vetted. When TSA has identified derogatory information that does not clearly support denial or revocation of a credential or other authorized access to transportation but warrants further investigation, the TSA's Encounters &

Analysis Branch[19] may review open source information, including publicly available social media, to ascertain whether there is information that may have a bearing on TSA's determination. TSA's review of social media is conducted pursuant to DHS Management Directive 110-01, *Privacy Policy for Operational Use of Social Media*.[20]

## 2.4 Discuss how accuracy of the data is ensured.

TSA relies on the individuals submitting their information and their employers to ensure the accuracy of the data. The DAC that aggregates the information on behalf of airport workers ensures that biometric and biographic information is correctly matched. Master personnel lists shared with TSA by the aircraft operators are expected to be accurate. An individual has an opportunity to review and correct errors before submitting information to TSA or correct inaccurate information during the process of resolving a credential denial or revocation. If the individual believes that he or she received a denial or revocation based on inaccurate information submitted to or obtained by TSA, the individual can seek redress. The redress process is explained further in Section 7 below.

## 2.5 Privacy Impact Analysis: Related to Characterization of the Information

**Privacy Risk:** There is a risk that an applicant may be incorrectly identified as a match to information contained in intelligence databases or to an individual listed in the centralized database of airport badge revocations.

**Mitigation:** TSA mitigates this risk by requiring data elements that should be sufficient to distinguish an applicant from individuals whose information is included in a derogatory data set or who are identified as a match to information contained in intelligence databases. TSA will further mitigate the risk of misidentification by requiring the applicant to certify the accuracy, to the best of his or her knowledge, of the PII submitted to TSA. TSA further mitigates this risk through the redress process for credential denials and revocations and through redress provided by the airport for any individuals listed in the revocation database.

**Privacy Risk:** There is a risk that individuals may be entered into the centralized database who have had their credential revoked for reasons other than, or unrelated to, failure to comply with aviation security requirements.

**Mitigation:** The privacy risk is mitigated by the database submission procedures and limiting access to the database. TSA provides strict instructions limiting the submission of

[19] *See* DHS/TSA/PIA-039 Encounters and Analysis Branch (October 12, 2017), *available at* https://www.dhs.gov/privacy.
[20] DHS Management Directive 110-01, Privacy Policy for Operational Use of Social Media, *available at* https://www.dhs.gov/privacy.

revocations only to those involving a failure to comply with aviation security requirements. Before an individual may be entered into the database, the airport operator must establish an administrative process to adjudicate the revocation for final disposition. Writeable access to the database will be limited to airport security coordinators or managers and TSA administrators responsible for maintaining the database. Finally, technical security controls such as password protection and username for log-in will be in place.

**Privacy Risk:** There is a risk that an individual's ability to be employed at an airport may be negatively impacted by inclusion in the centralized database.

**Mitigation:** This risk is partially mitigated. Individuals have the opportunity to challenge their inclusion in the database. Additionally, airport and airline operators are instructed that information contained in the centralized database does not prohibit an individual from being hired (for example, in a position that does not require unescorted access to a secure area).

# Section 3.0 Uses of the Information

## 3.1 Describe how and why the project uses the information.

The information is collected to conduct STAs on individuals seeking or holding authorized airport access or airport identification badges or credentials, as well as identification credentials or badges recognized by TSA under 49 CFR Parts 1542 and 1544, and non-traveling individuals requiring unescorted access to the Sterile Area of the airport to ensure he or she does not pose, and is not suspected of posing, a threat to transportation or national security. Once the airport badge or access to sensitive information is granted, individuals are recurrently vetted against law enforcement, immigration, and intelligence databases. TSA expects to leverage existing technology within TVS to host the centralized database.

TVS provides a person-centric view of applicants. TSA may be able to identify potential security risks that might otherwise not be readily apparent. For example, TVS will identify individuals who may attempt to conceal their true identity behind multiple names or aliases. It will also identify whether an individual has applied for multiple credentials. Rejection for one credential is not, by itself, grounds for rejection for another credential. TVS also provides the capability for TSA to identify links among applicants, such as whether multiple unrelated applicants share a common or false address.

The national centralized database will be used by airport and aircraft operators to document an individual's failure to comply with aviation security requirements and the revocation of the credential.

### 3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No, technology is not used to conduct electronic searches, queries, or analyses to discover or locate a predictive pattern or an anomaly. TVS does provide a capability to identify links across its populations, and thus identify anomalies such as multiple identities or links among applicants, but it does not identify predictive patterns or anomalies.

### 3.3 Are there other components with assigned roles and responsibilities within the system?

When SIDA applicants need access to areas of the airport controlled by the U.S. Customs and Border Protection (CBP), the individual will notify the DAC. The DAC will then locate the individual's SIDA application so that TSA can forward the application to CBP for adjudication as to the CBP area.

Applicant information may be shared also with U.S. Citizenship and Immigration Services (USCIS) for immigration status checks.

TSA transmits all airport worker fingerprints and associated biographic information to DHS's OBIM for enrollment into IDENT for recurring checks against immigration, terrorism, and law enforcement databases.

### 3.4 Privacy Impact Analysis: Related to the Uses of Information

**Privacy Risk:** There is a risk that information may be disclosed to individuals without a need to know or for unauthorized purposes.

**Mitigation:** This risk is mitigated by TSA's use of layered privacy safeguards that include physical, technical, and administrative controls to protect personal information in the automated system, appropriate to its level of sensitivity. These controls place limitations on the collection of PII, and protect PII against unauthorized sharing, use, modification, or destruction. System users receive privacy training and the system managers were involved in the drafting of this PIA.

**Privacy Risk:** There is a risk that anomalies discovered during the STA process may result in an inappropriate decision that negatively impacts the individual.

**Mitigation:** This risk is mitigated by requiring a secondary review of any anomaly using available data to ensure the accuracy of information obtained during the vetting process, as well as administrative and redress procedures that permit the individual to challenge the decision.

# Section 4.0 Notice

## 4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Airport and aircraft operators are required to provide a Privacy Act Statement to individuals at the time they submit their information for vetting by TSA. Individuals must certify in writing that all information provided is true, complete, and correct, and must acknowledge that a false statement or material omission can be punished by fine or imprisonment or both, and may be grounds for TSA to determine that the individual is ineligible. Individuals must acknowledge in writing that there is a continuing obligation to report an event or condition that makes the individual ineligible.

Airport operators are required to provide notice of the centralized database to all applicants at the time they apply for or renew any airport-issued ID media (badge or credential). The airport operators must provide a list of aviation security requirements and a notice that violations may result in their inclusion in the centralized database for five years from the date the violation occurred. If a badge is revoked, the airport operator must notify the individual of the reason why and that the individual's record is being entered into the database, as well as provide an opportunity to challenge the revocation.

The publication of this PIA and the applicable SORNs also serve to provide public notice of the collection, use, and maintenance of this information.

## 4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Individuals may elect not to provide information; however, doing so may delay the processing of their STA or prevent its completion. Individuals do not have the ability to limit uses of the information.

Individuals do not have the opportunity for consent regarding the national centralized database because inclusion for an aviation security violation is a legal requirement; however, the individual may seek correction through the redress process described in Section 7.

## 4.3 Privacy Impact Analysis: Related to Notice

**Privacy Risk:** Individuals may not be aware of vetting via IDENT.

**Mitigation:** Notice of sharing biographic and biometric information with IDENT for recurring checks against immigration, terrorism, and law enforcement databases was provided in a previous iteration of PIA and is provided in this PIA. The Privacy Act Statement provided to

individuals at the time they submit their information also gives express notice that TSA will conduct recurrent checks as part of the STA.

**Privacy Risk:** There is a risk that individuals may not know they will be entered into the centralized database if their credential is revoked for failure to comply with aviation security requirements.

**Mitigation:** This risk is mitigated. Airport operators must provide applicants with a list of aviation security requirements, and notice that revocation due to violations thereof may result in their inclusion in the centralized database for five years from the date the violation occurred. In addition, individuals must be provided notice before they are listed and given an opportunity to challenge their inclusion.

## Section 5.0 Data Retention by the Project

### 5.1 Explain how long and for what reason the information is retained.

TSA will retain information for one year after an individual's credential or access privilege granted based upon the STA is no longer valid. In addition, for those individuals who may originally have appeared to be a match to a government watch list, but are subsequently cleared as not posing a threat to transportation or national security, information will be deleted or destroyed seven years after completion of the STA, or one year after any credential or access privilege granted based on the STA is no longer valid, whichever is longer. Information contained in the subject database on individuals that are actual matches to a government watch list or otherwise pose a threat to transportation or national security, will be deleted or destroyed 99 years after completion of the STA, or seven years after TSA learns that the individual is deceased, whichever is shorter.

TSA expects to maintain centralized database records for five years in keeping with the time period that STAs are considered valid for aviation workers. TSA is seeking NARA approval of its proposed records disposition schedule.

### 5.2 Privacy Impact Analysis: Related to Retention

**Privacy Risk:** There is a risk that information used to conduct STAs will be retained longer than necessary.

**Mitigation:** This risk is mitigated. TSA will retain these records in accordance with the records retention schedule approved by NARA. TSA will delete the individual's information one year after it is notified by the airport that the individual's access is no longer valid which accomodates seasonal workers and provides flexibility for the individual. Individuals originally identified as a possible match but subsequently cleared will have their information retained for

seven years in order to provide the maximum opportunity for redress or review. The retention schedule is implemented through an automated daily sweep of the records.

**Privacy Risk:** There is a risk that individuals may remain in the centralized database for longer than necessary.

**Mitigation:** This risk is currently not fully mitigated as TSA is seeking NARA's approval for this records retention schedule. However, TSA expects to maintain individual records in the centralized database for five years from the date the violation occurred. Because STAs expire in five years, individuals who have had a credential revoked for failure to comply with aviation security requirements must undergo a new STA. TSA will automate the records disposal process so that all records are automatically deleted according to schedule.

## Section 6.0 Information Sharing

### 6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

The information will be shared with airport and aircraft operators and their service providers who aggregate individual information to provide to TSA. The information will be shared with the FBI for criminal history records checks and with the Terrorist Screening Center (TSC) to resolve potential watch list matches. Applicants who must undergo a fingerprint-based CHRC will have their information enrolled with the FBI's NGI for recurrent checks and Rap Back services for immediate notification of changes in criminal history. TSA also may share the information it receives with federal, state, or local law enforcement, immigration or intelligence agencies, or other organizations, in accordance with the routine uses identified in the applicable Privacy Act systems of records notices (SORN), DHS/TSA-002 Transportation Security Threat Assessment System (TSTAS) or DHS/TSA-019 Secure Flight Records for non-traveler checks.

TSA will also share information with the Social Security Administration (SSA) in order to confirm the validity of the SSN provided by the individual. Individuals will be asked to expressly authorize the SSA to confirm the validity of the SSN.

The centralized database is expected to increase information sharing between airport and airline operators. Before issuing a credential or badge, the airport operator must query the database to determine if an applicant has previously had a credential or badge revoked for violations of security regulations.

### 6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

All sharing of information outside the Department is compatible with the original collection. The purpose of the sharing is to facilitate the discovery of threats to the transportation system and to help prevent additional threats. Sharing of information outside of DHS is covered by DHS/TSA-002, specifically routine uses I, K, M, and N:

I. To an appropriate federal, state, local, tribal, territorial, or foreign agency regarding individuals who pose, or are suspected of posing, a risk to transportation or national security.

K. To a federal, state, local, tribal, territorial, or foreign agency, if necessary to obtain information relevant to a DHS/TSA decision concerning the initial or recurrent security threat assessment; the hiring or retention of an employee; the issuance of a security clearance, license, endorsement, contract, grant, waiver, credential, or other benefit; and to facilitate any associated payment and accounting.

M. To third parties during the course of a security threat assessment, employment investigation, or adjudication of a waiver or appeal request, to the extent necessary to obtain information pertinent to the assessment, investigation, or adjudication.

N. To airport operators, aircraft operators, maritime and surface transportation operators, indirect air carriers, and other facility operators about individuals who are their employees, job applicants or contractors, or persons to whom they issue identification credentials or grant clearances to secured areas in transportation facilities when relevant to such employment, application, contract, training, or the issuance of such credentials or clearances.

Sharing of information regarding non-travelers seeking access to the secured area is covered by routine use (3) in DHS/TSA-018 Secure Flight Records, and compatible with the purpose for the original collection:

> (3) To aircraft operators, foreign air carriers, airport operators, the Department of Transportation, and the Department of Defense or other U.S. Government agencies or institutions to communicate individual screening status and facilitate an operational response (where appropriate) to individuals who pose or are suspected of posing a risk to transportation or national security.

### 6.3 Does the project place limitations on re-dissemination?

No, the program does not place limitations on re-dissemination beyond the protections of the Privacy Act of 1974. Information shared with state and local agencies, and with employers, operators, and owners of transportation facilities or assets is typically limited to the result of the STA, which must be disseminated for operational purposes, including issuance of a credential and

permitting access to facilities or assets.

TSA does not place limitations on re-dissemination by the TSC except to the extent match information is Sensitive Security Information (SSI).[21] Re-dissemination of SSI is limited by SSI regulation.[22]

### 6.4 Describe how the project maintains a record of any disclosures outside of the Department.

Disclosures are recorded manually within investigative files or automatically in an output report. In addition, TIM maintains an electronic log of all data sharing transactions.

### 6.5 Privacy Impact Analysis: Related to Information Sharing

**Privacy Risk:** There is a risk that information will be inappropriately shared.

**Mitigation:** TSA mitigates this privacy risk by sharing information within DHS to only those with a need to know in the performance of their official duties, and externally only in accordance with published routine uses under the applicable system SORN. Further, TSA has entered into a Memorandum of Understanding (MOU) with the FBI and TSC governing the conditions of sharing information related to STA programs.

## Section 7.0 Redress

### 7.1 What are the procedures that allow individuals to access their information?

Individuals covered by the Privacy Act (PA) or the Judicial Redress Act[23] may request access to their data by contacting the TSA Freedom of Information Act (FOIA) Branch:

Transportation Security Administration
TSA-20
FOIA Branch
601 South 12th Street
Arlington, VA 20598-6020

FOIA/PA requests may also be submitted by email at FOIA@tsa.dhs.gov. The FOIA/PA request must contain the following information: full name, current mailing or email address, and telephone number, and specific information about the records sought. Please refer to the TSA FOIA web site

[21] 49 U.S.C. § 114(r).
[22] 49 CFR Part 1520.
[23] The Judicial Redress Act (JRA) provides covered persons with a statutory right to make requests for access and amendment to covered records, as defined by the JRA, along with judicial review for denials of such requests.

at www.tsa.gov for further instructions. Access may be limited pursuant to exemptions asserted under 5 U.S.C. § 552a(k)(1) and (k)(2).

If an individual wishes to appeal his or her STA, he or she may request the records upon which TSA's determination was based. Instructions detailing how to request the records are included in the individual's eligibility determination notification.

### 7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

In the case of criminal history records checks adjudicated by employers, if an individual applying for a credential disputes the results of a CHRC (i.e., that the disposition of a charge/s) is incorrect, the applicant can provide court documentation to his or her employer's security office. If the applicant can show that the disposition (or charge) does not fall under the disqualifying offense category, he or she can be granted a credential. If the applicant can show that corrected disposition or charge no longer falls under the disqualifying offense category, he or she can be granted a credential. NOTE: The employer's security office will need to contact TSA (the CHRC requestor) to verify with the FBI that the court record has been changed in favor of the applicant.

Individuals who believe that they have been wrongly identified as a security threat will be given the opportunity to contact TSA to address their concerns. Redress based on the name-based portion of the security threat assessment will be handled on a case-by-case basis due to the classified and/or SSI that may be involved. TSA will provide information on which the determination was based to the applicant to the extent permitted by law. There may be items that are classified or SSI that cannot be released. Individuals who believe that their immigration status check determination is inaccurate should contact USCIS to address their concerns.

Direct employees and authorized representatives of U.S. aircraft operators who are not U.S. Citizens and reside overseas may seek redress by contacting the U.S. Department of State (DOS) Consular Section of the nearest U.S. Embassy or Consulate in his or her country of residence. The individual will be asked to provide identifying information as well as sign a statement authorizing TSA to conduct to a background investigation. The U.S. Embassy will securely transmit the information to the DOS and the appropriate country desk. The appropriate TSA representative will be copied. The DOS will initiate the redress procedure through TSA. TSA will coordinate the response internally and coordinate with appropriate U.S. federal intelligence and law enforcement to determine whether any relief can be provided to the individual. TSA will ask the U.S. Embassy to inform the individual's host government and the individual of TSA's conclusion. In addition, a companion letter will be drafted for the TSA Administrator's signature informing the air carrier of the determination. DOS will send the approved cable to the Embassy and TSA will send the letter via express mail to the airline.

Airport and aircraft operators will be required to notify individuals of their placement in

the centralized database along with the reason for the revocation, and must establish administrative processes that permit the individual an opportunity to correct their record or seek expungement.

### 7.3 How does the project notify individuals about the procedures for correcting their information?

STA adverse notifications sent directly to the individual include the appropriate procedures for appealing or requesting a waiver. This PIA also provides redress information.

### 7.4 Privacy Impact Analysis: Related to Redress

**Privacy Risk:** An airport worker might have his or her credential revoked for reasons other than failure to comply with aviation security requirements and be entered into the centralized database.

**Mitigation:** Airports will be required to establish an administrative process to determine whether a violation of an aviation security requirement has been substantiated and a redress process to allow an individual whose record is mistakenly entered into the database to correct the record and have the individual's record expunged from the database.

**Privacy Risk:** No redress is available for non-traveling individuals who seek and are denied unescorted access to secured areas of airport because of an erroneous potential match to a terrorist watch list.

**Mitigation:** Non-traveling individuals who fail the watch list check will be denied entry to the secured area of airport. The airport operator may decide to allow *escorted* access but otherwise there is no immediate opportunity for the individual to resolve the error. This risk is partially mitigated by the individual's opportunity to correct his or her record afterwards through DHS's Traveler Redress Inquiry Program (TRIP).[24]

## Section 8.0 Auditing and Accountability

### 8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

TSA information systems are protected by systems of passwords, restricted access, and other measures to mitigate the risk of unauthorized access to sensitive information. TSA system administrators, security administrators, IT specialists, vetting operators, and analysts have access to the system in order to perform their duties in managing, upgrading, and using the system. Contractors hired by TSA to perform IT maintenance and security monitoring tasks have access to the systems to perform their official duties. Additionally, TSA may use contract adjudicators to

[24] *See* DHS/ALL/PIA-002(b) DHS Traveler Redress Inquiry Program (TRIP), (April 23, 2018), *available at* https://www.dhs.gov/privacy.

review STA information. All contractors performing this work are subject to requirements for suitability and a background investigation.

Role-based access controls are employed to limit the access of information by different users and administrators based on the need to know the information for the performance of their official duties. TSA also employs processes to enforce separation of duties, to prevent unauthorized disclosure, or to prevent modification of information. No unauthorized users are permitted access to system resources.

TSA expects to create a secure portal to TVS through which airlines will submit their data for recurrent vetting. TSA expects the small airports to be able to submit their employee PII through this portal once established as well. Aircraft operators must provide their TSA Principal Security Inspector (PSI) with a 24-hour/7 day-a-week point of contact. This individual, usually the security manager or coordinator, is required to have an STA including a CHRC and will be responsible for submitting the names of airline direct employees and authorized representatives to TSA, monitoring submissions, and resolving any issues or concerns that arise regarding the submission of data. TSA will establish a secure registration process and access procedures to the portal for individuals responsible for submitting the PII to TSA.

### 8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All TSA and contractor personnel are required to complete on-line privacy training, which includes instructions on handling PII. Compliance with this requirement is audited by the TSA Privacy Office. In addition, TSA provides security training, which helps to raise the level of awareness for protecting personal information being processed.. Individuals accessing the system must have any necessary background investigations and/or security clearances for access to sensitive information or secured facilities based on TSA security policies and procedures. Furthermore, TSA adjudicators go through extensive training prior to assuming responsibility for reviewing case files. They are subject to close monitoring and peer review and must consistently meet performance standards for accuracy and timeliness.

### 8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

All access requests are submitted in writing to the TIM Program Manager/System Owner, who grants access and designates a system administrator to provide access to approved individuals. Access to any part of the system is approved specifically for, and limited only to, users who have an official need to know the information for the performance of their duties associated with the STA process. External storage and communication devices are not permitted to interact with the

system. All access to and activity within the system are tracked by auditable logs. Audits will be conducted in accordance with TSA Information Security guidelines.

### 8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

New information sharing, uses, or access will be controlled in accordance with Sections 8.2 and 8.3, and will be reviewed for compliance with the applicable SORN and this PIA. All MOUs are reviewed by the program manager, TSA Privacy Office, and Chief Counsel before submitting to DHS for formal review.

## Responsible Officials

Sonya Badgley, Project Manager
Transportation Security Administration
Department of Homeland Security

## Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____

Dena Kozanas
Chief Privacy Officer
Department of Homeland Security

# Appendix

## STA components for Aviation Worker populations

| Population/Program | Function/Access | Intelligence Databases | Crim History Record Check | Immigration Databases |
|---|---|---|---|---|
| Airport Workers w/SIDA, sterile area, or secured area access | Direct airport employees including employees of vendors at airport requiring unescorted access to SIDA, Sterile or secured area of airport. | X | X | X |
| Airport Workers | Direct airport employees, employees of vendors at airport, taxi drivers, parking lot attendants, and shuttle bus drivers, who do NOT require unescorted access to SIDA or sterile area. | X | Not required | X |
| Airport Badging Personnel | Direct airport employees responsible for issuing airport badges and credentials. | X | X | X |
| Airport Security Managers/Coordinators (including Category IV airports) | Direct airport employees responsible for airport security program and for maintaining, updating and submitting personnel lists to TSA. | X | X | X |
| Aircraft Operator Workers (airline employees including all-cargo) | Flight crewmembers, individuals with screening functions, and those with authority to perform checked baggage or cargo functions. | X | X | |

| | | | | |
|---|---|---|---|---|
| Aircraft Operator Workers NOT issued a SIDA | Direct airline employees not covered by an airport Security Directive or issued an airport badge such as reservation agents but perform security functions or have access to Sensitive Security Information (SSI). | *X | | |
| Air Cargo Screeners w/sterile area or secured area access | Individuals employed by TSA-certified cargo screening facilities and screen cargo, supervise cargo screening, have access to screened cargo, act as security coordinator or alternates, or are senior managers of the facility in control of operations. | X | X | X |
| Indirect Air Carriers (IAC) w/ sterile area or secured area access | Individuals employed by entities that use aviation indirectly to transport cargo by air and have unescorted access to cargo, access to information that cargo will be transported by air, unescorted access to cargo screened for transport on passenger aircraft, or who perform certain functions related to the transporation, dispatch, or security of cargo transported on passenger aircraft or all-cargo aircraft. | X | X | X |

| | | | | |
|---|---|---|---|---|
| Master Crew List (MCL) | A list of domestic and international air carriers' flight crew members that TSA has vetted and determined do not pose a security threat and are authorized to fly to, from, or over the United States and its territories. | X | | |
| Public Area Airport Workers | Some airports issue badges or credentials to individuals who work in the public area; e.g., taxi drivers. | X | | X |
| Non-traveling Individuals Accessing Regulated Areas of Airport | Members of the public, short-term maintenance or other service providers, including those *escorted* to and within the SIDA. | *X | | |
| Direct employees of CAT IV airports without badging systems. | Small airports without a SIDA that do not issue badges. | *X | | |
| Private Charter Standard Security Program (PCSSP) | Private charter flight crewmembers using aircraft with a maximum certified take-off weight of greater than 100,309.3 pounds. | *X | X | |
| Twelve-Five Standard Program (TFSSP) | Flight crew members employed by aircraft operators using aircraft with a maximum certified take-off weight of 12,500 pounds or greater. | *X | X | |
| Airspace Waivers | Flight crewmembers and armed security officers operating on domestic and foreign aircraft that request a waiver to enter areas of restricted airspace, including | X | | |

| | | | | |
|---|---|---|---|---|
| | overflights of the United States and its terrortories. | | | |
| Alien Flight Student Program | Aliens and other designated candidates seeking flight instruction or recurrent training on certain aircraft at FAA-regulated flight schools in and outside of the United States. | X | X | X |
| DCA Access Program | All flight crewmembers and armed security officers on aircraft flying in and out of National Airport (DCA). | X | X | |
| Maryland-3 Program | Private pilots flying to, from, or between the 3 general aviation airports closest to the National Capital Region, and their airport security coordinators. | X | X | |
| *No Fly/Selectee portion of intelligence database check currently conducted by the airport or aircraft operators but will transition to TSA | | | | |